Simulating Smart Grid Cyber Security

Abdul Razaq, Huaglory Tianfield
Glasgow Caledonian University

Bernardi Pranggono
Sheffield Hallam University

Hong Yue
Strathclyde University

Contents

Abbreviations

AMI	Advance Metering Infrastructure
API	Application Program Interface
DDoS	Distributed Denial-of-Service
DoS	Denial-of-Service
DSSS	Direct Sequence Spread Spectrum
FHSS	Frequency-Hopping Spread Spectrum
HMI	Human Machine Interface
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IPC	Inter-Process Communication
IPS	Intrusion Prevention System
KF	Kalman Filter
LFC	Load Frequency Control
LSM	Load Signature Moderation
MITM	Man-In-The-Middle attack
MTU	Master Terminal Unit
OLE	Object Linking and Embedding
PCB	Printed Circuit Board
PG	Power Grid
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PLL	Phase Lock Loop
PMU	Phasor Measurement Unit
PSS	Power System Simulation
QoS	Quality of Service
RED	Random Early Detection, for network scheduler
RF	Radio Frequency
RPC	Remote Procedure Calls
PSLF	Positive Sequence Load Flow
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SEG	Smart Energy Gateway
SG	Smart Grid
SoS	System of Systems

SSIDS	Synchrophasor Specific Intrusion Detection System

1. Introduction

Power Grid (PG) is a complex system, consisting of massive hardware components, and their continuous monitoring and control. What's more, real-time responsiveness further demands access within the installation vicinity as well as remote access. The integrity of Supervisory Control and Data Acquisition (SCADA) in Smart Grids (SGs) should ensure that only legitimate and authorized actions are permitted to access the critical components, e.g., Master Terminal Unit (MTU), Remote Terminal Unit (RTU), Programmable Logic Controller (PLC), relay, transformer, switch, etc.

Information and Communications Technology (ICT) plays a fundamental communication role underpinning SG's various functional systems, which automate local and remote tasks, perform even-driven responses and execute various management processes, etc. This intensive use of cyber infrastructure presents serious complications, with respect to security and integrity of physical system as well as with the ICT subsystem. Alternative current is a product of dangerous system that should be handled with a strict set of precautions. A breach in such a delicate system from physical fabric or ICT can cause severe consequences, including interruption of electricity, equipment damage, data breach, complete blackouts or life threating consequences.

SGs are exposed to a broad range of security threats from generators to providers and from distributors to consumers. A SG consists of two sets of technologies, namely power electronics and ICT that are integrated as one system fulfilling one goal, i.e., "uninterruptable and cost effective energy supply." Today, the security focus in SG has to be expanded to include withstanding the disruptions caused not only by physical but also cyber-attacks.

A comprehensive cyber security framework for SG is required to address the vulnerabilities presented in these two distinct layers. This holistic security infrastructure should protect and address the complete system from generation to transmission networks for appropriate voltage and frequency with distribution of electricity, depending upon consumption requirements.

2. Power Grid Being a Cyber-Physical System

At the physical level, the performance of power grid depends on the physical devices and the environment. Therefore, devices should be designed to sustain adverse environmental factors [1] and possible brutal force attacks. MTUs and RTUs of SCADA system controlling PLCs from generation to transmission systems require strict timing to control the demand and supply of electricity. Automation in SG is realised with SCADA system. SCADA devices are physical part of the power grid for real-time control and monitoring in substations and main-station. As illustrated in Figure 1, a SCADA system consists of Human Machine Interface (HMI), which is part of MTU. MTU is used to monitor RTU, which is connected to PLC for automation [2]. Data communication between RTUs and MTU occurs over wired lines or wireless technologies.

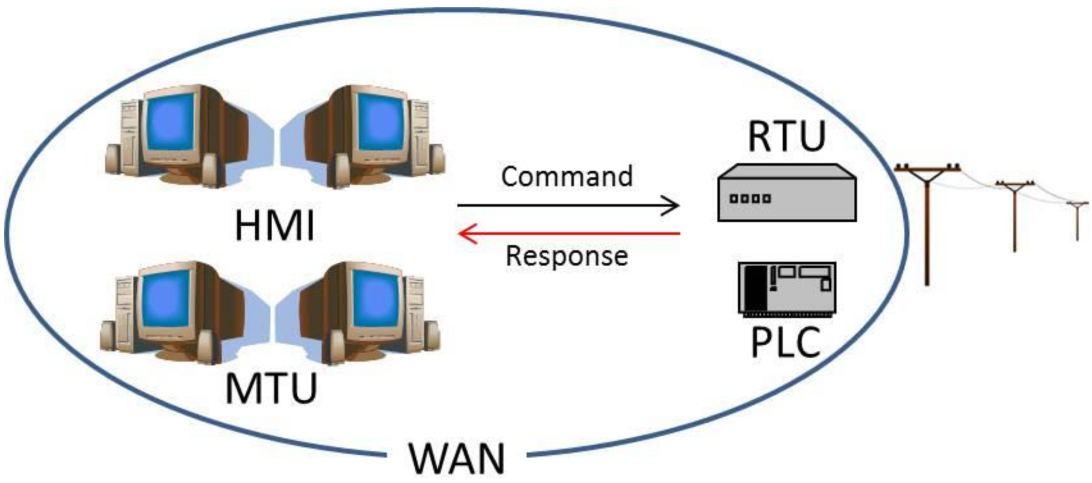

Figure 1. SCADA system

SCADA devices are real-time or non-real-time small computer systems that each manipulate its electrical outputs based on the condition of electrical input signals and program logic [2]. These controllers are usually connected to devices such as pumps, valves, drives (motors), thermometers, and tachometers, etc. SCADA devices manage simple to complex systems, from a few to thousands of nodes. These systems are capable to interact with components in real-time or near real-time. Timed response to initiated request is very important because any delay in the operation can result in drastic events. Measuring local signals of short-circuit relays are considered between 4 to 40 ms for immediate response to local grid. Such systems are widespread in utility industries including water, gas and electricity and play a vital role to automate and monitor geographically dispersed sites. Historically, individual companies developed their own proprietary hardware and operating software based on various vendors. Interoperability was often not a requirement which made security least important as these devices were meant to operate in confined and closed networks [3].

In the era of Internet connectivity, where aggregated data needs centralized analysis such as big data technologies and cloud platforms, these systems are insufficiently designed to handle challenges posed by openness and omnipresence.

Security of interconnected devices and subsystems is important but it should not result in a degraded and unreliable system. Communication in distributed devices and applications should satisfy security constraints including device authentication, data confidentiality, message integrity and prevention mechanism to withstand cyber-attacks. Historically, control in industrial automation was done mechanically with hydraulic controllers or manually [4]. These mechanical components were upgraded once electronics such as transducers, relays and hard-wired control circuits became available. This changed to new dimensions, when small microcontrollers were introduced, allowing smaller size and the ability to connect over wire or wireless links. This evolution paved a way for complete digital systems that were able to control and monitor remotely, which required communication protocols. These communication protocols are commonly referred to as fieldbus protocols.

Various protocols and technologies are used in traditional power grids for communication purpose such as Modbus, Modbus+, profiBus, ICCP, DNP3, PROFINET, INTERBUS, WorldFIP, etc. It is worth noting that all of these protocols were designed without considering cyber security variable. Existing deployed communication protocols were developed under the standardisation umbrella of IEEE, IEC and DNP3. IEC 60870-5 and DNP3 are considered the most widely used protocols in automation industry. IEC is typically used in European countries and recognized by IEEE 1379 standard, which is used in Asia and North America [1].

The automation in SG inherits security challenges and vulnerabilities because most of the systems were not designed to be open but accessible only at installation facilities [5]. Beside the design limitations in SCADA devices, the IT itself poses real challenges as real-time performance and continuous operation in power grid cannot use general purpose IT architecture and devices. The majority of existing software solutions and hardware components were, produced for isolated installations without security concerns, deployed in independent and isolated environments. However, with the network connectivity, which is the intrinsic design aspect of SG, these software and hardware solutions have to go through iterative process of re-engineering with security and exposure to outer world for dependent and connected settings.

Intensive use of cyber infrastructure presents serious complications to physical system as well as to ICT subsystem [1, 6]. Efficiency, reliability and security of interconnected devices and systems are critical for enabling SG communication infrastructures. Interoperability must be achieved while systems are not being isolated into non-competitive technical solutions or the complete existing power and communication systems need to be replaced [7]. Protection mechanism should be adopted at all stages of energy demand-supply chain as security is a fundamental building block; thus, prevention should serve as a last resort to critically defend against any possible intrusion [8]. Secure SG will not only have the ability to withstand contingencies and avoid energy blackouts, but also ensure uninterruptable energy with service reliability [9].

Smart grid is exposed to threats at different stages of energy demand-supply chain, as illustrated in Figure 2. Smart Grid is a System of Systems (SoS), consisting of various independent components. Securing each component is important; however, challenges occurring from a whole SoS are even more serious. Imagine multiple systems are combined nonlinearly and non-deterministically and this may generate an uncertain outcome. For example, the power consumption signature of a single household may propagate to full-scale power-house production. Transition from traditional power grids to intelligent SoS is a drastic shift with systems integration to combine physical and remote infrastructure using ICT [10].

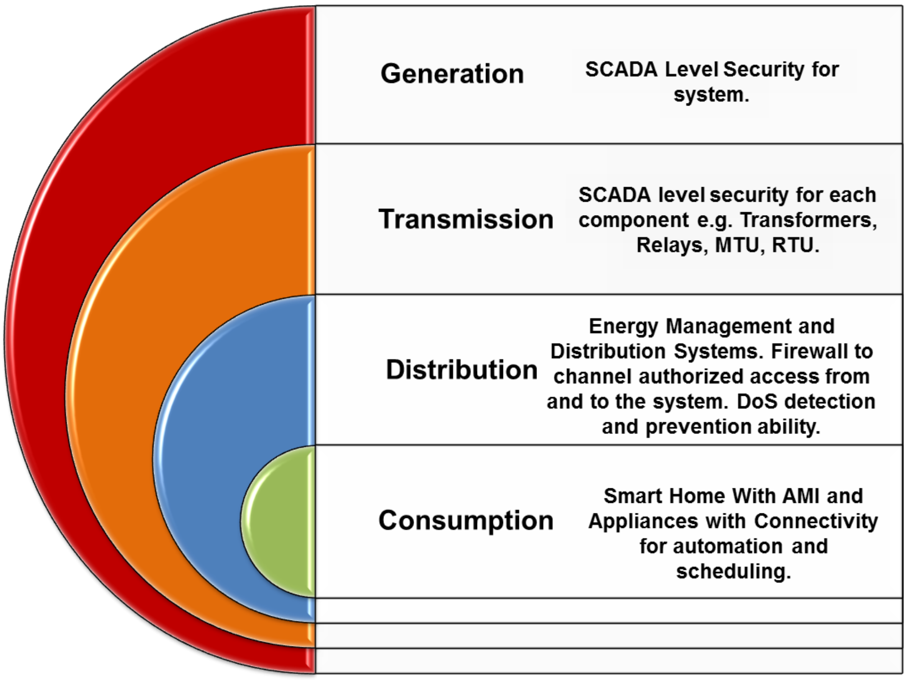

Figure 2. Security requirements at different stages of energy demand-supply chain

3. Cyber Security Threats and Vulnerabilities

Security, by definition, represents a safe state of an individual or entity from physical and virtual vulnerabilities. Security in ICT domains, also known as cyber security, refers to the practices adopted to acquire the state of safety in which computers, networks and communications protocols operate. Privacy defines the liberty of individuals to sustain their identity without being exposed. In ICT, this is referred to the ability of individuals, selectively sharing their identities with the systems, servers, networks, applications, etc., without compromising security. In power and energy domains, security can be defined as the system's capability to withstand disturbances such as system fault or unanticipated loss of system elements due to natural or human causes. In smart grid, the security focus of the industry has expanded to include withstanding disturbances caused by man-made physical and cyber-attacks.

Figure 3 illustrates how cyber infrastructure is constructed in support of SG connectivity. Generation, transmission and distribution are underpinned with wide-area network (WAN) topologies, while building area network (BAN) allow the grouping of houses together before being interfaced to advanced metering infrastructure (AMI) in home area network (HAN), which is typically implemented in local area network (LAN) topology settings.

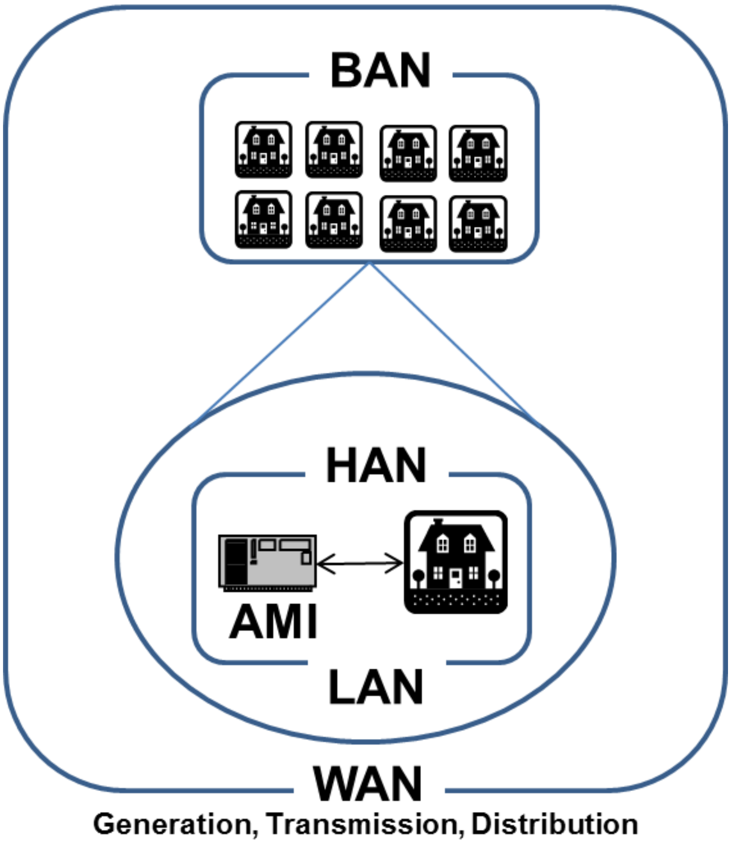

Figure 3. Smart grid cyber infrastructure

Cyber security for SG is of immense concern because of emerging cyber-threats and security incidents targeting critical infrastructure such as SGs all over the world. These threats are severe if SG systems are deployed without appropriate security plan and measurements.

In 2000, millions of liters of raw sewage were spilled out into local parks and rivers due to a series of cyber-attack from a disgruntled employee in Queensland, Australia gaining unauthorized access into a computerized management system. The access has been made possible by installing company software on the employee's personal laptop and infiltrating the companies' network to take control of the waste management system [11].

In 2003, Safety Parameter Display System and Plant Process Computer System at Davis-Besse nuclear power plant in Ohio, in the US had been successfully attacked and disabled by the Slammer worm. The worm entered the plant network by a contractor's infected computer that was connected via telephone dial-up directly to the plant network, thus bypassing the firewall [11].

In 2010, the Stuxnet worm attacked the Siemens SIMATIC WinCC SCADA system, using at least four vulnerabilities of the Microsoft Windows operating system [12]. It was the first malicious code attack which damaged the industrial infrastructures directly. According to Symantec's statistics, about 45,000 networks around the world have been infected with the worm so far, and 60% of the victim hosts are in Iran [13]. Stuxnet has become the first worm crossing both the cyber and physical world by manipulating the control system of the critical infrastructure.

In 2012, Flame [14] infiltrated and transferred data from thousands of computers in the Middle East including biggest oil and gas company by counterfeiting an official Microsoft security certificate in the form of a Microsoft update. Flame is more sophisticated compared to Stuxnet. Although Flame is designed for spying not destruction, the damage it caused is comparable or more. The high-flexibility of Flame also possesses great possibility to deploy it as cyber-attack tool for critical infrastructure.

Stuxnet, Flame and Duqu [15] malwares indicate the tendency of cyber-wars and terrorism in the future. It also means that cyber-security must be inherently embedded into any critical infrastructure network as a foundation of next generation critical infrastructure. Stuxnet showed us that security-by-obscurity concept has serious loopholes which can be exploited.

Recently a bug termed as 'Heartbleed' [16] in OpenSSL has initiated a debate in the research community seeking security measures and re-assessment of user grade software solutions for multibillion national assets, such as power grids.

Existing security approaches are unscalable, incompatible, or simply inadequate to address the challenges posed by highly complex environments such as SG [17]. The NIST has established coordination task group and European Network and Information Security Agency (ENISA) also published recommendations for member states on SG cyber security [18]. Cyber-security threats in SG can be categorized as disclosure, integrity, denial-of-service (DoS), and cloning. Every key system in SG is vulnerable to these risks.

Smart Grid Cyber Attacks

With SG being piloted all over the world, it is necessary before standardization that efficient and secure infrastructure in terms of devices, network protocols and software applications must be developed. Implementation of SG will deploy automated devices with real time control. These deployed devices utilize at least one of the connectivity such as RF or wire media to form a communication layer. A secure layer serves as a first line of defence, however, what happens on that transport media presents a set of challenges. A comprehensive cyber security framework for SG is required to address the vulnerabilities from connecting media to information exchanged over this very channel. Generally cyber-attacks in power grids can be categorized into three categories [2]:

- Attack on the hardware: such as changing value in automation devices, RTU and HMI. Typically, it is aimed to control a smart grid device and an initial step of a bigger attack with main objective to control the whole system.

- Attack on software: such as exploiting vulnerabilities in commonly used DNP3 and Modbus protocols. Similar to hardware attack, typically it is aimed to control a smart grid device and an initial step of a bigger attack with main objective to control the whole system.
- Attack on network topology: exploiting network topology vulnerability, such as DoS attack, overflowing an RTU with protocol messages, etc. It is aimed to overwhelm the communication and/or computational resources resulting in delay or communication failure.

These cyber-attacks are based on the exploitation of vulnerabilities present in the underlying computer and networking technologies. Table 1 summarises techniques for cyber protection.

Table 1. Protection Techniques Against Cyber-Attacks

Solutions	**Limitations**	**Suggestions**	**Comments**
PKI – Identity Check, cryptography	Not possible for resource limited devices such as smart meters, PLCs and devices without internet connectivity	With simple connections devices can utilize cloud resources	Latency because of network and prone to other network attacks.
SN - Physical sensor network to monitor the nodes	Expensive solution with high maintenance requirement	Install on micro-grid level or top of hierarchy	Maintenance cost with typical hardware failure problems
FH - Frequency Hopping to avoid Jamming	Prone to ghost reads and not feasible for devices without variable Phase Lock Loop (PLL), and requires extensive overhead for sync	Higher frequencies with lower output power (dB) can reduce the effective range.	Suggested method can reduce the probability but it is vulnerable to original threats.
Service Port Switching – Similar to FH	Extensive sync overhead and requires dynamic port assigning	Sync overhead can utilize cloud resources with virtual access only	Dynamic port switching not feasible solutions for resource limited devices. Poor QoS with huge sync overhead
Blocking – black listing	Problem with DDoS as source signature will change	Suitable for systems with dedicated IP/Signatures	Applications hosted in cloud with geo-location can't use this technique.
KF - Kalman Filter for hardware or software solution	Requires high end hardware to execute complicated recursive algorithms.	Must be considered as front line of defence.	Typical IDS/IPS solution with comprisable QoS
Network/Request Scheduler – Random Early Detection (RED) and variants, packet drop.	Not feasible for devices with hardware limitation. QoS is always questionable	Virtual implementation in cloud before passing the control commands to equipment	Similar problem as with KF solution

In general, the cyber security threats in SG can be classified in terms of the traditional confidentiality, integrity, and availability (CIA) triad.

Confidentiality

This type of threats involves the user's privacy and utility providers' business secrets. Imagine an adversary is able to monitor AMI traffic, which will allow to reasonably estimating the users' behavior and schedule, steal business secrets involving the load estimates, distribution blue-prints, security credentials, etc. AMIs and components using Radio Frequency (RF) as a communication media means they are prone to typical RF eavesdropping, whereas hard-wired components such as computers, routers, switches, etc., are prone to LAN sniffer attacks. It is also worth noting that RF communication is prone to RF jamming. The data exchange between each component should have end-to-end encryption. Physical components should be shielded sufficiently, so the communication occurring on hardware links can be protected.

Liu et al. [5] investigated jamming attacks targeted at physical Load Frequency Control (LFC) device in SG while analyzing dynamic performance of communication channels connected to RTUs in power systems. Case-studies of simulated congested attacks were modeled as a switched (ON/OFF) power system and two-area LFC theoretical model was built for different attack-launching instants. It has been concluded that adversaries can make power system unstable via DoS attacks if communication channels of RTUs are jammed. Similar work by Liu et al. [1] investigated jamming threat but for wireless networks in the power systems. They suggested that traditional anti-jamming techniques such as Frequency-Hopping (FH), Frequency-Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) can serve the purpose with additional measurements. A test-bed implementing Micaz motes in ZigBee network were simulated and theoretical analysis was presented to demonstrate proposed intelligent local controller switching. ZigBee networks implement AES algorithm to protect their confidentiality. Furthermore, frame integrity is protected through the integrity codes utilization [19].

Integrity

Malicious software (malware) can compromise the system and result in devastating effects. Cyber integrity in smart grid should guarantee that only legitimate and authorized actions are permitted to access the critical components, such as SCADA systems, utility business secrets, and user private data. An unauthorized or mistaken access to RTU can lead to shocking results from destruction of physical infrastructure, such as PLCs, to rerouting the electricity on under-prepared transmission networks.

The cloning threat is unauthorized access/service being executed with legitimate credentials. The AMI is an ideal target for such threat, cloning a fake meter ID, which can cheat the reporting and billing mechanisms. A cloned meter ID can allow attackers to consume the electricity with no charges while, accumulating the consumption to target AMI assignee. Replicating the ID on resource limited hardware is relatively convenient as it normally requires overwriting the unique ID stored in flash memory, so the system should be capable of detecting the dual ID detection and use physical shielding to prevent the Printed Circuit Board (PCB) being exposed.

Man-in-The-Middle (MITM) attack is arguably the most common attack in this category. In this attack the adversary intercepts network data (e.g, breaker and switch states) and meter data from remote terminal units, modifies part of these, and forwards the fabricated version to the control center. In the absence of data alerts in the modern power systems, the hacker could succeed to modify both network and meter data elaborately such that they are consistent with the target topology. The impact of MITM attack on smart grid SCADA system has been demonstrated by Yang et al. [20].

Lu et al. [9] reviewed the security threats involving network availability, data integrity and information reliability, and evaluated their feasibility and impact on the SG. They suggested that pseudo identity attacks can lead to a phase transition phenomenon in the delay performance of the communication protocol and that shorter packets can be more resistant to such attacks. Huang et al. [21] studied the impact of bad data injection attack in smart grids. They investigated a detailed problem formulation and the quickest techniques to detect a bad data injection attack.

Manandhar et al. [22] looked into theory of false data injection attacks in power systems and proposed a solution based on Kalman Filter (KF). They suggested these attacks can be averted with linear quadratic estimation detectors for sensors in SG such as Phasor Measurement Units (PMU) which measure current phase and amplitude in power systems. The projected values by KF and incoming instant values can be compared to detect an anomaly in the system. Yang et al. also investigated the impact of cyber-attacks on PMU [23]. They simulated MITM and DoS attacks against a practical synchrophasor system to validate the effectiveness of the proposed Synchrophasor Specific Intrusion Detection System (SSIDS).

Availability

DoS is a typical phenomenon to block the service with illegitimate requests, while lingering or sometimes even denying the service to authentic users. The actual blocking can last for a long period, therefore, the requested action is never executed, or it can delay the required action long enough to make it useless or even harmful. This attack not only affects the end users by depriving them from electric power, but also presents extreme threats to utility providers. MTUs, controlling PLCs to generation or transmission systems, require strict timing to control the demand and supply of electricity. These systems are normally located in remote locations, as the name suggests. A penetration in the system to block the access to MTU can result in disastrous physical results.

He et al. [6] have proposed a mechanism based on MicaZ and TelosB motes to resist DoS attacks against adversaries and legitimate insiders. They argued that Public Key Infrastructure (PKI) is a viable solution for uninterruptible service; however, deployment of PKI is directly proportional with cost for large scale networks such as SG. Different security protocols have been suggested depending upon the applications' scalability and resources on board.

Sgouras et al. [7] presented a qualitative assessment of DoS attacks with simulation in OMNeT++ and INET framework. They examined performance of AMIs, routers and utility servers under such situation. An attack on AMI would result in minor consequences connected to single entity whereas similar scenarios for utility server would cause drastic effects during peak hours. Similar work was conducted by Yi et al. [8] to demonstrate the impact of DoS in ICT without involving power grid simulation. Their work is mainly focused on AMI with ns-2 simulator. They termed their DoS attack as puppet attack which would penetrate in the system like worm and continue to congest the communication channels with false data until the network is exhausted.

4. Simulating Smart Grid Cyber Security

A coherent cyber security framework is required to support both domains of SG, namely, power grid and ICT, with their specific requirements. Existing simulation systems can be used to some extent to evaluate cyber security in SG; however, these simulators are not specifically designed for this purpose.

Cyber security simulation has been under-developed, although existing simulators do provide limited coverage of cyber security. Cyber security simulator should consist of comprehensive protection framework because smart grid is indeed a system of systems, consisting of various independent components across the different stages of the energy demand-supply chain.

Simulating complex systems like SG may requires ways of handling multiple simulation processes, e.g., cascade and inter-process. In cascade method, output of one simulation is used to initiate second simulation; two processes run in separate process spaces. This can be also achieved by altering the application's settings file which application reads at regular intervals or on specified events. Object Linking and Embedding (OLE) is also a popular technique to embed one application in another. Cascade method is ideal for closed applications that do not provide access to source code.

Another method is to utilize Inter-Process Communication (IPC) which allows two processes communicating at runtime while exchanging the information in real-time. Common techniques for IPC include message exchange, shared memory, and Remote Procedure Calls (RPC). IPC is the classic method to possibly alter the application behavior at runtime without requiring source code and recompiling the binaries.

In general, there are two main approaches to simulating smart grid, i.e., simulators coupling for SG and dedicated single SG simulator.

Simulators Coupling for Smart Grid

The most common technique is coupling of simulators. Mets et al. [24] theoretically evaluated different solutions and proposed a solution based on commercial and open-source solution. A similar work is conducted by Li et al. with focus on communication network [25]. The work by Hopkins et al., termed EPOCHS, [26] can be tracked back as one of the early simulator for SG to combine communication with electric power components. EPOCHS is based on ns-2 and commercial power components; its flow is illustrated in Figure 4.

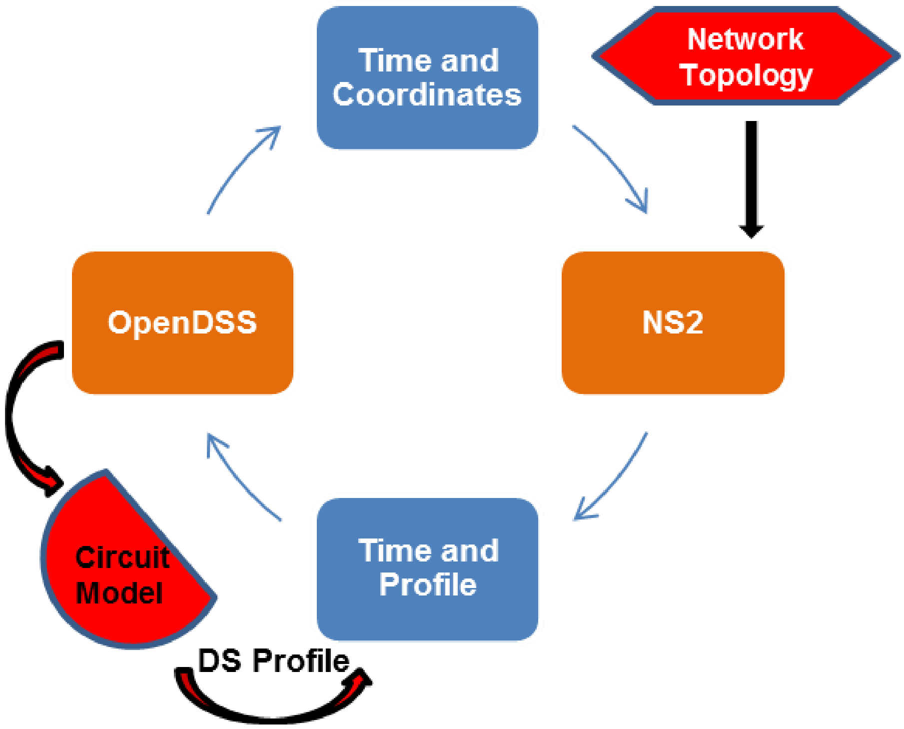

Figure 4. EPOCHS flow (adapted from [26])

Dugan et al. [27] demonstrated a simulator based on the work by Godfrey et al. [28] with hypothetical example using power distribution system and ns-2. Lin et al. [29] proposed GECO which used identical approach while utilizing the ns-2 and GE's Positive Sequence Load Flow (PSLF). The flow is illustrated in Figure 5.

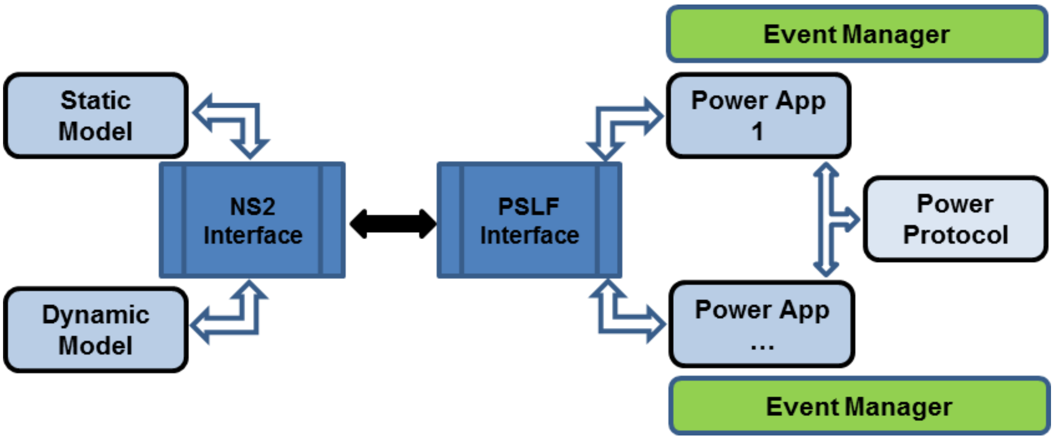

Figure 5. GECO flow (adapted from [29])

Chassin et al. [30, 31] utilized GridLAB-D and MatPower. Yan et al. [10] investigated communication interface of SG using ns-2 and OMNeT++. Both solutions have been used in cyber security domains and are best candidate to simulate communication cyber security. Hence, the existing network security solutions can be utilized and new dedicated solutions can be developed to meet the SG specific challenges where traditional enterprise network cyber security solutions do not work or apply. A general flow of ns-2 is depicted in Figure 6.

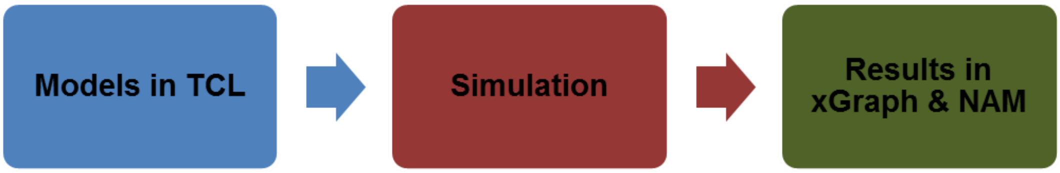

Figure 6. ns-2 flow

(Tcl, originally from Tool Command Language, is a scripting language. xGraph is a plotting program and Nam a Tcl/Tk based animation tool.)

The work by Anderson et al. [32], called GridSpice, is an interesting endeavour towards smart grid simulation. GridSpice employs a combination of GridLAB-D (Figure 7) and MatPower as its backend to simulate power distribution system [33]. Tan et al. [34] have employed a similar approach and have developed ScorePlus simulator for cyber-physical test-bed that addresses the intelligent control, communications, and interactions in smart grid. Bhor et al. [35] have presented a co-simulation system by means of a widely used power (OpenDSS) and network (OMNeT++) simulators, and authors claimed that time synchronization is resolved while providing a framework for continuous and event-based requirements. A similar work is conducted by Xinwei et al. [36] using OpenDSS as power simulator and OPNET for network simulation.

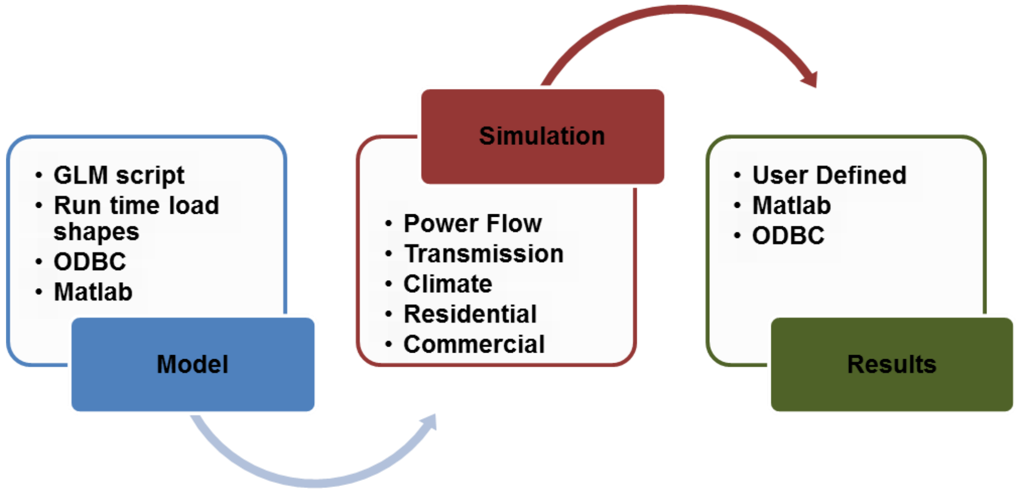

Figure 7. GridLAB-D flow

(GLM - GridLAB-D Model, ODBC - Open Database Connectivity)

In all existing solutions to simulators coupling for smart grid, security is not explicitly addressed.

Dedicated Single Smart Grid Simulator

A very intuitive work by Zhou et al. [37] has resulted InterPSS for Power System Simulation (PSS). Although it is not meant to address security issues but this solution has a great potential for SG security. Chinnow et al. extended the InterPSS with their own simulator called Network Security Simulator (NeSSi^2) [38]. Their main focus is smart meter or AMI while providing the security paradigm for such infrastructure. In contrast to other popular network simulators, such as ns-2 [39], ns-3 [40] or OMNeT++ [41], *NeSSi^2* provides a comprehensive Application Programming Interface (API) for the integration and evaluation of Intrusion Detection System (IDS). Attack scenarios are relatively easy to simulate using *NeSSi^2*. It also provides methods to simulate smart grid networks by supporting both IP and energy networks.

Mets et al. [42] adopted the similar approach but with different toolkits, i.e., OMNeT++ for communications and MATLAB to model grid distribution. Gomes et al. [43] simulated partial functionality of smart grid based on agent-based model to understand consumption and distribution but not generation and transmission.

Table 2 summarises existing smart grid simulators.

Table 2. Smart grid simulators

SG Simulator	Constituent Power Simulator	Constituent Communication Simulator	Open-Source	Treatment of Cyber Security
Hybrid Simulator [27]	OpenDSS	ns-2	Yes	No
EPOCHS [26]	PSLF	ns-2	Partial	No
GECO [29]	PSLF	ns-2	Partial	Yes
Gridspice [32, 33]	GridLAB-D	N/A	Partial	No
SCORE [34, 44]	GridLAB-D	N/A	Yes	Yes
ScorePlus [35]	OpenDSS	OMNeT++	Yes	No

Co-Simulation Platform [36]	OpenDSS	OPNET	Partial	Yes
InterPSS [37]	Limited	No	Yes	No
NeSSi^2[38]	Limited	Limited	Yes	Yes
Integrated Simulation [42]	MATLAB	OMNeT++	Partial	Yes

5. Simulation of Denial-of-Service Attack in Smart Grid

A recent study by Baker *et al.* highlighted that nearly 80% of electrical enterprises in 14 countries were victims of large-scale distributed denial-of-service (DDoS) attacks [45]. Nearly 25 percent of the executives who were part of the study reported extortion through threatened or realized cyber-attacks. This was a 20 percent increase as compared to the year before. Smart meters will be deployed on a large-scale in a short time and the study emphasizes the critical issue regarding the security of such systems. Several schemes have been proposed to implement smart grid privacy, including Anonymous Credential, 3rd Party Escrow Architecture, Load Signature Moderation (LSM), ElecPrivacy, Smart Energy Gateway (SEG) and privacy preserving authentication [46]. The study in [47] focused on comparing the approaches and architectures aimed at protecting the privacy of smart grid users.

In this section, we demonstrate DoS attack simulation and the technique to tackle this type of attack. Our simulation uses NeSSi^2 due to its open-source license and ability to simulate power grid and IP networks as a single application. NeSSi^2 is scenario and profile based simulation tool. Each network in NeSSi^2 consists of at least one scenario which is eventually profiled depending upon required simulation. A scenario defines a type of profiles that can be deployed on each node of the network. Multiple profiles can be deployed on single node within a single scenario. Profile is a component to provide a set of functionalities incorporating single or various features related to power grid and IP network simulation, which can be deployed onto SG nodes. Finally, profiled scenario requires a simulation component which allows the mapping of power and network domains while linking the corresponding entities. NeSSi^2 is capable to generate various attack scenarios and traffic analysis.

Figure 8 depicts the high level topology of the SG simulation, (a) Power grid and (b) the corresponding IP network. The power grid consists of one generator and two consumption subnets representing insecure and secure grid configurations. The IP network also consists of similar topology with the server as the main subnet connected to insecure and secure subnets. The mapping between power grid and IP network is configurable at node level within the simulation.

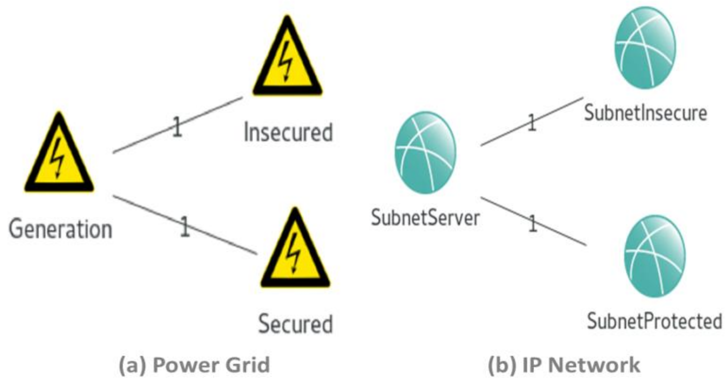

Figure 8. Smart grid network topology

Figure 9 depicts a more detailed configuration of the power grid of Figure 8(a). The power grid consists of green generation based on solar panel with output of 5147W. Placed between generation and consumption are two step-down transformers with varying current of 380kV to 220kV, which represent transmission and distribution. These swing bus profiled transformers are eventually connected to two consumption local grids: “Secure” and “Protected.” As solar generation is considered unreliable, dependent on the surrounding environment, a swing bus is used between the links from solar panel to transmission transformer. Swing bus accommodates system losses by emitting or absorbing active/reactive power to/from the system. Transformer connected to insecure subnet is profiled with line failure profile to simulate the load unavailability during power interruption simulation. Line failure profile of NeSSi^2 allows simulating the load unavailability in target power line between required time intervals. This line failure profile only accepts a link line, and cannot be mapped to consumption node, because only a single line can be mapped in each instance of application. Consumption subnets further consists of one transformer and two smart houses. These smart houses are capable to simulate load consumption and are mapped to the corresponding IP nodes in the IP network for communication simulation. Smart houses are capable to emulate load usage depending upon time, weather and number of persons.

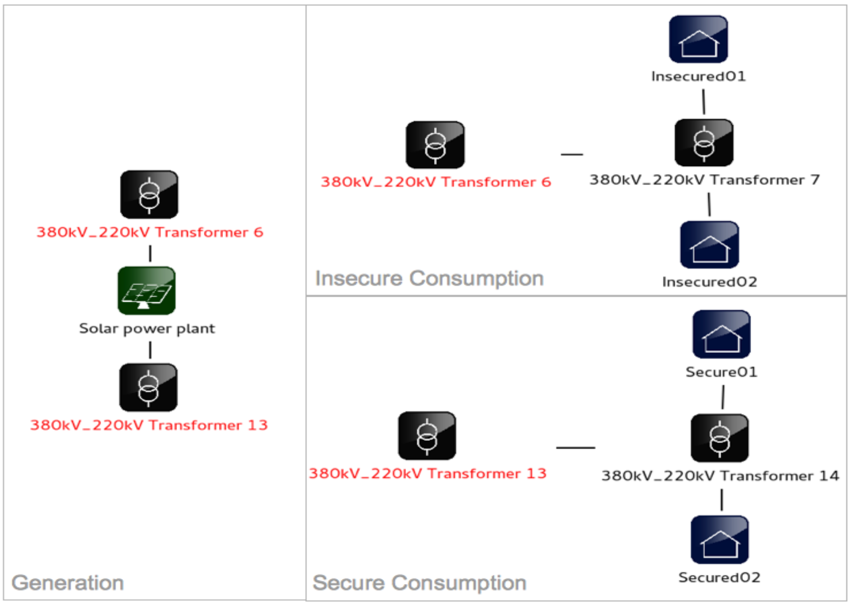

Figure 9. Power grid layout

Figure 10 depicts the configuration of a 100Mbps IP network. The main subnet or server subnet is connected to two subnets labelled as "Insecure Subnet" and "Secure Subnet." The server node with "Server Subnet" is profiled as Echo server application serving both connected subnets.

The server subnet is connected to the insecure subnet without any protection mechanism in place, whereas the secured subnet is connected via front-end firewall. Moreover, the secured subnet deploys additional firewall at client's interface level in case the router has been compromised by malicious activity. DoS attacks simulated via BOT component are presented in both the insecure and the secure subnets. The firewall alone is not sufficient solution; an Intrusion Prevention System (IPS) along with IDS must be carefully designed and deployed side-by-side to protect critical infrastructure such as smart grid [34]. NeSSi^2's firewall and packet sniffer profiles are very limited, which results in restricted functionality.

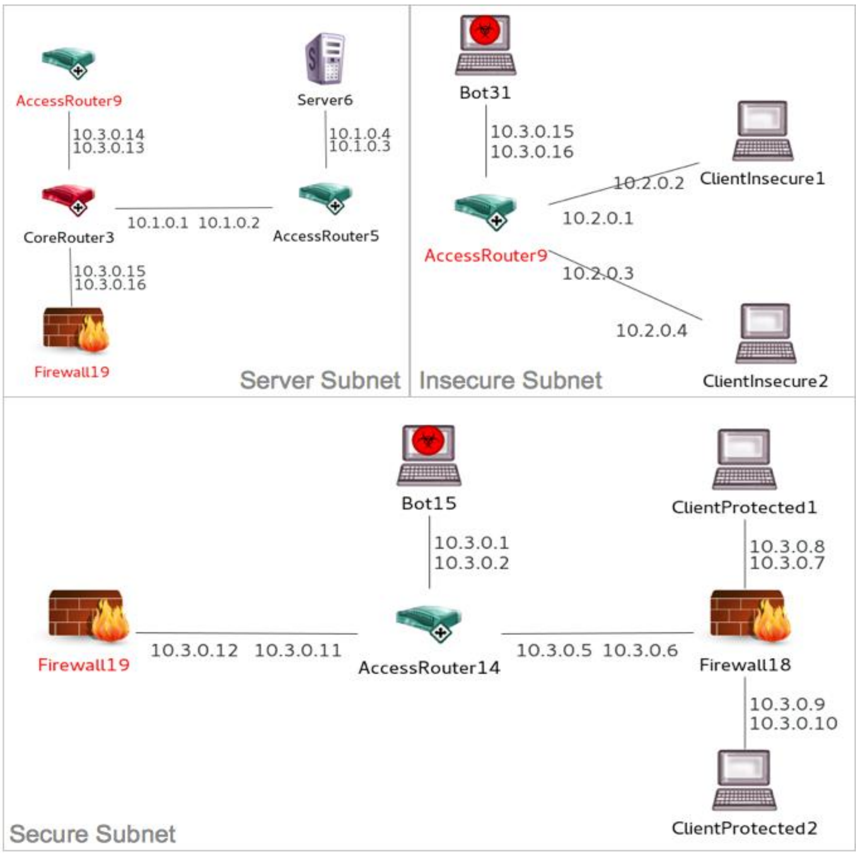

Figure 10. IP network layout

All nodes of the IP network are configured with default load (echo client/server) at the beginning of simulation. Packet flow on IP links is increased from default load to demonstrate the packet loss which replicates the DoS attack. DoS or inability to serve the legitimate incoming requests is a phenomenon where system's capacity reaches its maximum throughput and prompts unavailability of a given service. The ability to handle DoS attacks is crucial due to power grid's strict availability requirements. Botnet attack is emulated in both secure and insecure networks for DoS attack. The BOT profile in $NeSSi^2$ is limited to only specifying the attack start time and only targeting single IP node. All these IP nodes are mapped to smart houses in the power grid with one-to-one relationship, which means that a house in the power grid has a counterpart IP client in the IP network.

This simulation is executed over 1000 ticks and failure or interruption of electricity and communication is simulated between 105-350, 500-600 and 800-900 ticks (time intervals), respectively. A tick is the smallest possible time interval (event) in $NeSSi^2$. The actual duration depends on the simulation, the simulation mode and the underlying hardware platform. The solar panel model is set to produce 5147W peak production whereas smart houses are simulated for 5 persons each with 0.90% consumption of the received load.

Figure 11 presents the simulation statistics of 1000 tick of the server's echo response to the secure and the insecure subnet nodes. The vertical axis represents the communication packets whereas the horizontal axis represents numbers of the ticks or the simulation time itself. Interruption of the insecure subnet is visible between failed intervals with a lower density of packets compare to tick intervals for the secure subnet.

Communication of the insecure client is presented in Figure 12. The packet drop statistics marked with cyan colour simulates the failure scenario when the client was under attack from BOT and failed to process the echo packets. Successful echo request is marked in yellow colour whereas packets in magenta colour represent the forwarded packets. The successful and drop packets can be compared with server's statistics which illustrates fewer packets during the failed communication of the insecure client. The failed intervals can also be cross-checked in Figure 13 which presents the load statistics of the insecure smart house. The mapping between the insecure client and the smart house is carried out prior to the simulation and the smart house is profiled with the smart house consumption profile along with the line failure profile at the transformer link level. The corresponding IP client is profiled with the echo client and the device failure.

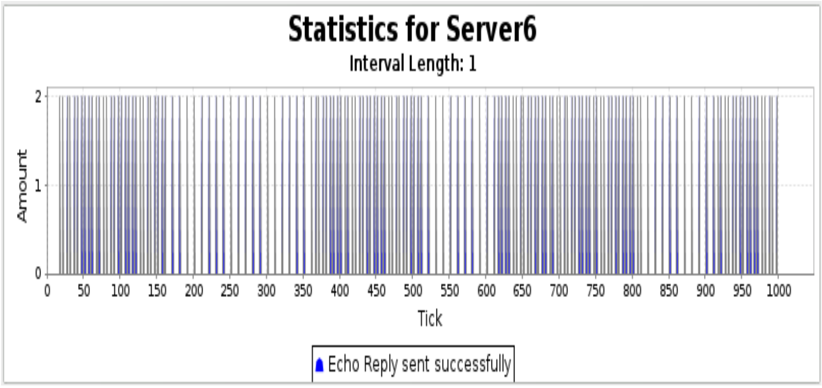

Figure 11. Server communication - Secure and Insecure subnets

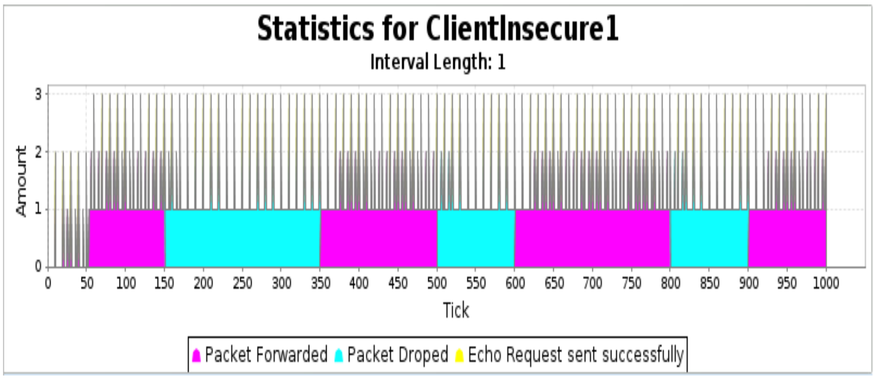

Figure 12. Insecure IP client

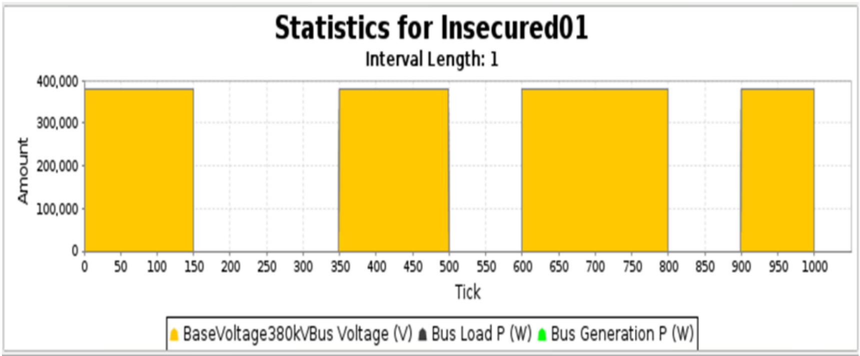

Figure 13. Power interruption of the insecure house

6. Open Issues

Smart grid is seen as a potential solution to future energy challenges. Integration with ICT is fundamental to meeting the environmental-friendly, reliable and resilient electricity requirements.

None of current SG simulators has put cyber security issues as its main focus. Developing a SG simulator needs to assess and evaluate the smart grid's reliability and cyber security across all the interdependent aspects such as power sub-systems, automation, and communication networks. A smart grid cyber security simulator also needs to effectively simulate the interactions among the different components within the SG.

Another challenge is the quantity of data that SG may generate. The data come from various nodes with various timestamps and serving different purposes This undoubtedly needs a platform to handle the big data challenges.

References

[1] H. Liu, Y. Chen, M. C. Chuah, and J. Yang, "Towards self-healing smart grid via intelligent local controller switching under jamming," in *2013 IEEE Conference on Communications and Network Security (CNS),*, 2013, pp. 127-135.

[2] W. Dong, L. Yan, M. Jafari, P. M. Skare, and K. Rohde, "Protecting Smart Grid Automation Systems Against Cyberattacks," *IEEE Transactions Smart Grid, on,* vol. 2, pp. 782-795, 2011.

[3] M. Erol Kantarci and H. T. Mouftah, "Energy-Efficient Information and Communication Infrastructures in the Smart Grid: A Survey on Interactions and Open Issues," *IEEE Communications Surveys & Tutorials,,* vol. 17 , , pp. 179 - 197, 2015.

[4] H. Farooq and L. T. Jung, "Choices available for implementing smart grid communication network," in *2014 International Conference on Computer and Information Sciences (ICCOINS),*, 2014, pp. 1-5.

[5] S. Liu, X. P. Liu, and A. E. Saddik, "Denial-of-Service (dos) attacks on load frequency control in smart grids," in *2013 IEEE on Innovative Smart Grid Technologies Conference (ISGT),*, 2013, pp. 1-6.

[6] D. He, S. Chan, Y. Zhang, M. Guizani, C. Chen, and J. Bu, "An enhanced public key infrastructure to secure smart grid wireless communication networks," *IEEE Network,,* vol. 28, pp. 10-16, 2014.

[7] K. I. Sgouras, A. D. Birda, and D. P. Labridis, "Cyber attack impact on critical Smart Grid infrastructures," in *2014 IEEE Innovative Smart Grid Technologies Conference (ISGT),*, 2014, pp. 1-5.

[8] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and J. Li, "A denial of service attack in advanced metering infrastructure network," in *2014 IEEE International Conference on Communications (ICC),*, 2014, pp. 1029-1034.

[9] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid," in *2010 Military Communications Conference (MILCOM 2010)*, 2010, pp. 1830-1835.

[10] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Communications Surveys & Tutorials,,* vol. 14, pp. 998-1010, 2012.

[11] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "SCADA security in the light of Cyber-Warfare," *Computers & Security,* vol. 31, pp. 418-436, 2012.

[12] T. M. Chen and S. Abu-Nimeh, "Lessons from Stuxnet," *Computer,* vol. 44, pp. 91-93, 2011.

[13] N. Falliere, L. O. Murchu, and E. Chien., "W32. Stuxnet dossier. Symantec Security Response," 2011.

[14] K. Munro, "Deconstructing Flame: the limitations of traditional defences," *Computer Fraud & Security,* vol. 2012, pp. 8-11, 2012.

[15] B. Bencsáth, G. Pék, L. Buttyán, and M. Félegyházi, "Duqu: Analysis, Detection, and Lessons Learned," in *ACM European Workshop on System Security (EuroSec)*, 2012.

[16] M. Carvalho, J. DeMott, R. Ford, and D. A. Wheeler, "Heartbleed 101," *IEEE Security & Privacy,,* vol. 12, pp. 63-67, 2014.

[17] H. Jingfang, W. Honggang, and Q. Yi, "Smart grid communications in challenging environments," in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm),*, 2012, pp. 552-557.

[18] E. Egozcue, D. H. Rodriguez, J. A. Ortiz, V. F. Villar, and L. Tarrafeta, "Smart Grid Security - Recommendation for Europe and Member States," ENISA 2012.

[19] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," *IEEE Communications Magazine,,* vol. 51, pp. 42-49, 2013.

[20] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, E. G. Im, Z. Q. Yao*, et al.*, "Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in Smart Grid SCADA systems," in *International Conference on Sustainable Power Generation and Supply (SUPERGEN 2012),*, 2012, pp. 1-8.

[21] Y. Huang, M. Esmalifalak, H. Nguyen, R. Zheng, Z. Han, H. Li*, et al.*, "Bad data injection in smart grid: attack and defense mechanisms," *IEEE Communications Magazine,,* vol. 51, pp. 27-33, 2013.

[22] K. Manandhar, C. Xiaojun, H. Fei, and L. Yao, "Combating False Data Injection Attacks in Smart Grid using Kalman Filter," in *2014 International Conference on Computing, Networking and Communications (ICNC),*, 2014, pp. 16-20.

[23] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, B. Pranggono, P. Brogan*, et al.*, "Intrusion Detection System for network security in synchrophasor systems," in *IET International Conference on Information and Communications Technologies (IETICT 2013),*, 2013, pp. 246-252.

[24] K. Mets, J. Ojea, and C. Develder, "Combining Power and Communication Network Simulation for Cost-Effective Smart Grid Analysis," *IEEE Communications Surveys & Tutorials,,* vol. PP, pp. 1-26, 2014.

[25] W. Li, M. Ferdowsi, M. Stevic, A. Monti, and F. Ponci, "Cosimulation for Smart Grid Communications," *IEEE Transactions on Industrial Informatics,,* vol. 10, pp. 2374-2384, 2014.

[26] K. Hopkinson, X. Wang, R. Giovanini, J. Thorp, K. Birman, and D. Coury, "EPOCHS: a platform for agent-based electric power and communication simulation built from commercial off-the-shelf components," *IEEE Transactions on Power Systems,,* vol. 21, pp. 548-558, 2006.

[27] R. Dugan, S. Mullen, T. Godfrey, and C. Rodine, "Hybrid simulation of power distribution and communications networks," in *Proceedings of the 21st International Conference on Electricity Distribution (CIRED'11)*, 2011.

[28] T. Godfrey, S. Mullen, R. C. Dugan, C. Rodine, D. W. Griffith, and N. Golmie, "Modeling Smart Grid Applications with Co-Simulation," in *2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm),*, 2010, pp. 291-296.

[29] H. Lin, S. S. Veda, S. S. Shukla, L. Mili, and J. Thorp, "GECO: Global Event-Driven Co-Simulation Framework for Interconnected Power System and Communication Network," *IEEE Transactions on Smart Grid,,* vol. 3, pp. 1444-1456, 2012.

[30] D. P. Chassin, K. Schneider, and C. Gerkensmeyer, "GridLAB-D: An open-source power systems modeling and simulation environment," in *2008 IEEE Transmission and Distribution Conference and Exposition (T&D)*, 2008, pp. 1-5.

[31] D. P. Chassin, J. C. Fuller, and N. Djilali, "GridLAB-D: An Agent-Based Simulation Framework for Smart Grids," *Journal of Applied Mathematics,* vol. 2014, p. 12, 2014.

[32] K. Anderson, J. Du, A. Narayan, and A. El Gamal, "GridSpice: A distributed simulation platform for the smart grid," in *2013 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES),*, 2013, pp. 1-5.

[33] K. Anderson, J. Du, A. Narayan, and A. El Gamal, "GridSpice: A Distributed Simulation Platform for the Smart Grid," *IEEE Transactions on Industrial Informatics,,* vol. PP, pp. 1-1, 2014.

[34] S. Tan, W.-Z. Song, L. Tong, and Y. Wu, "Integrated Software Testbed for Cyber-Physical Analysis in Smart Grid," in *Innovative Smart Grid Technologies Conference (ISGT 2014)*, Washington, DC, 2014.

[35] D. Bhor, K. Angappan, and K. M. Sivalingam, "A co-simulation framework for Smart Grid wide-area monitoring networks," in *Sixth International Conference on Communication Systems and Networks (COMSNETS 2014)*, 2014, pp. 1-8.

[36] S. Xinwei, C. Ying, L. Jiatai, and H. Shaowei, "A co-simulation platform for smart grid considering interaction between information and power systems," in *2014 IEEE Innovative Smart Grid Technologies Conference (ISGT),*, 2014, pp. 1-6.

[37] M. Zhou and Z. Shizhao, "Internet, Open-source and Power System Simulation," in *2007 IEEE Power Engineering Society General Meeting,*, 2007, pp. 1-5.

[38] J. Chinnow, K. Bsufka, A. D. Schmidt, R. Bye, A. Camtepe, and S. Albayrak, "A simulation framework for smart meter security evaluation," in *2011 IEEE International Conference on Smart Measurements for Future Grids (SMFG),*, 2011, pp. 1-9.

[39] ns-2. (2013, 10/12/2013). *The Network Simulator - ns-2*. Available: http://www.isi.edu/nsnam/ns/

[40] G. Riley and T. Henderson, "The ns-3 Network Simulator," in *Modeling and Tools for Network Simulation*, K. Wehrle, M. Güneş, and J. Gross, Eds., ed: Springer Berlin Heidelberg, 2010, pp. 15-34.

[41] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," in *1st international conference on Simulation tools and techniques for communications, networks and systems & workshops*, Marseille, France, 2008, pp. 1-10.

[42] K. Mets, T. Verschueren, C. Develder, T. L. Vandoorn, and L. Vandevelde, "Integrated simulation of power and communication networks for smart grid applications," in *16th IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD 2011)*, 2011, pp. 61-65.

[43] L. Gomes, P. Faria, H. Morais, Z. Vale, and C. Ramos, "Distributed, Agent-Based Intelligent System for Demand Response Program Simulation in Smart Grids," *IEEE Intelligent Systems,,* vol. 29, pp. 56-65, 2014.

[44] S. Tan, W.-Z. Song, D. Huang, Q. Dong, and L. Tong, "Distributed Software Emulator for Cyber-Physical Analysis in Smart Grid," *IEEE Transactions on Emerging Topics in Computing,,* October 2014.

[45] S. Baker, N. Filipiak, and K. Timlin. (2011, April). In the dark: Crucial industries confront cyber-attacks. *McAfee 2nd annual critical infrastructure protection report*. Available: http://www.mcafee.com/cip

[46] F. Siddiqui, S. Zeadally, C. Alcaraz, and S. Galvao, "Smart Grid Privacy: Issues and Solutions," in *21st International Conference on Computer Communications and Networks (ICCCN 2012)*, 2012, pp. 1-5.

[47] S. Zeadally, A.-S. Pathan, C. Alcaraz, and M. Badra, "Towards Privacy Protection in Smart Grid," *Wireless Personal Communications,* vol. 73, pp. 23-50, 2013/11/01 2013.